UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

GHASSAN ALASAAD, NADIA ALASAAD, SUHAIB ALLABABIDI, SIDD BIKKANNAVAR, JÉRÉMIE DUPIN, AARON GACH, ISMAIL ABDEL-RASOUL aka ISMA'IL KUSHKUSH, ZAINAB MERCHANT, MOHAMMED AKRAM SHIBLY, MATTHEW WRIGHT, and DIANE MAYE ZORRI,

Plaintiffs,

v.

KEVIN McALEENAN, Secretary of the U.S. Department of Homeland Security, in his official capacity; JOHN SANDERS, Acting Commissioner of U.S. Customs and Border Protection, in his official capacity; and MATTHEW T. ALBENCE, Acting Director of U.S. Immigration and Customs Enforcement, in his official capacity,

Defendants.

Civil Action No. 17-cv-11730-DJC

Hon. Denise J. Casper

PLAINTIFFS' MEMORANDUM IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT

Adam Schwartz
Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)
adam@eff.org
sophia@eff.org
saira@eff.org

Esha Bhandari
Hugh Handeyside
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

Jessie J. Rossman
Matthew R. Segal
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
jrossman@aclum.org
msegal@aclum.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Other Authorities

INTRODUCTION

This case concerns the constitutionality of the government's warrantless and suspicionless searches of travelers' electronic devices at the U.S. border. The Defendants' policies expressly authorize border officers to conduct these searches without a warrant or probable cause, and usually without even reasonable suspicion. Such searches violate the First and Fourth Amendments to the U.S. Constitution.

Today's electronic devices contain vast quantities of highly personal information that the Supreme Court has repeatedly held requires a warrant to be searched in other contexts. *See Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The border search context is no different, because border searches of travelers' electronic devices equally intrude upon the "privacies of life." *Riley*, 573 U.S. at 403. The Fourth Amendment also prohibits confiscations of travelers' devices absent probable cause, for purposes of searching the devices after travelers leave the border.

Plaintiffs are ten U.S. citizens and one lawful permanent resident who were subjected to such invasive device searches—several of them on multiple occasions. The government also confiscated four of Plaintiffs' devices for lengthy periods. Plaintiffs seek injunctive and declaratory relief to prevent such searches and confiscations in the future, and to expunge the information the government has retained from past searches.

This case also implicates the constitutional rights of the broader traveling public. U.S. border officers searched the smartphones, laptops, and other electronic devices of more than 33,000 international travelers last year, almost four times the number from just three years prior. Border searches of electronic devices intrude deeply on the private lives of all travelers and raise unique concerns for the journalists, lawyers, doctors, and others who carry particularly sensitive information about their news sources, clients, and patients.

Warrantless and suspicionless device searches turn the border into a digital dragnet, where the government can search and retain troves of highly personal information about individuals—and their families, friends, and colleagues. The record demonstrates that this highly invasive practice is untethered from the immigration and customs enforcement rationales that have historically justified the government's warrantless and suspicionless search authority at the border. The government cannot use the border to circumvent the Constitution.

BACKGROUND

Plaintiffs filed their Complaint on September 13, 2017. *See* ECF No. 1, and Amended Complaint, ECF No. 7. Defendants moved to dismiss on December 15, 2017, arguing that Plaintiffs lacked standing and had failed to state cognizable claims. *See* ECF No. 14.

On May 9, 2018, this Court denied Defendants' motion to dismiss. On standing, this Court held that "Plaintiffs have plausibly alleged that they face substantial risk of future harm from Defendants' ongoing enforcement of their border electronics search policies," and that "Plaintiffs have plausibly demonstrated that expungement of their data would afford some redress for their alleged injury." Memorandum and Order, ECF No. 34 ("Mem. Ord.") at 24, 26. The Court also held that Plaintiffs plausibly stated Fourth Amendment claims against warrantless searches, *id*. at 45–46, and confiscations without probable cause, *id*. at 47. Lastly, the Court concluded that Plaintiffs have "plausibly alleged that the government's digital device search policies substantially burden travelers' First Amendment rights." *Id*. at 52.

All Plaintiffs now move for summary judgment against all Defendants on all claims.

SUMMARY OF UNDISPUTED MATERIAL FACTS[1]

Plaintiffs come from diverse backgrounds and occupations. They are a limousine driver, a nursing student, the operator of a security technology business, a NASA engineer, two journalists, an artist, the editor of a media organization, a filmmaker, a computer programmer, and a professor who formerly served as an Air Force captain. Plaintiffs' Statement of Undisputed Material Facts In Support of their Motion for Summary Judgment ("SUMF") ¶¶ 120, 124, 126, 128, 131, 133, 136, 143, 145, 148. Defendants subjected each Plaintiff to a warrantless search of their electronic device, and four Plaintiffs suffered multiple searches. *Id*. at ¶¶ 120–149.

Defendants have promulgated formal policies on searches of travelers' electronic devices at U.S. ports of entry. SUMF ¶¶ 1, 6, 17. U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE") allow border officers to conduct "basic," or manual, searches of travelers' devices with no suspicion, and "advanced," or forensic, searches with reasonable suspicion of activity in violation of the laws enforced or administered at the border. SUMF ¶¶ 9, 10, 18, 19. CBP also allows advanced searches based on a "national security concern," even without reasonable suspicion. SUMF ¶ 9. A "basic" search is one in which officers do not use external equipment to review a device's contents, while in an "advanced" search, officers connect external equipment to the traveler's device. SUMF ¶¶ 7, 8. Neither CBP nor ICE requires a warrant or probable cause for either type of search. In contrast, for other types of searches, CBP and ICE sometimes obtain warrants or apply a probable cause or reasonable suspicion standard. SUMF ¶¶ 103–119. For example, CBP and ICE are required to obtain warrants to open international mail in certain circumstances and to read correspondence in all

[1] Pursuant to Local Rule 56.1, the undisputed material facts supporting Plaintiffs' Motion are set forth in the accompanying Plaintiffs' Statement of Undisputed Material Facts.

circumstances, SUMF ¶¶ 106, 113, even though CBP claims authority to read the same type of correspondence on an electronic device without any suspicion whatsoever, SUMF ¶ 107.

Both CBP and ICE allow confiscation of devices for the purpose of searching them after travelers leave the border. Under CBP policy, confiscation "ordinarily" should not exceed five days but can be prolonged with a supervisor's approval. SUMF ¶ 11. ICE policy authorizes confiscation for a 30-day period that also can be extended with a supervisor's approval. SUMF ¶ 21. Neither agency sets any maximum time limit for device confiscations. SUMF ¶¶ 12, 21.

Defendants' policies permit them to retain information from a traveler's device if it is relevant to immigration, customs, and other enforcement matters. SUMF ¶¶ 13, 22. Both agencies' policies allow them to share this information with federal, state, local, and foreign law enforcement agencies. SUMF ¶¶ 14–16, 24. When CBP shares information from travelers' electronic devices with other government entities, it does not monitor whether those entities impermissibly retain it. SUMF ¶ 16.

Defendants' retention and sharing of information from border searches of electronic devices can increase the odds that a traveler will be subject to future device searches. When deciding whether to search a traveler's device, CBP and ICE officers may consider information about the traveler that is stored in their databases, which include TECS (CBP's main database for border screening), the Automated Targeting System ("ATS"), and ICE's Investigative Case Management. SUMF ¶¶ 25, 35, 36, 44, 48. The information stored in these databases may include the fact that border officers previously searched the traveler's device or subjected them to other screening, SUMF ¶¶ 5, 26, 34, 37, 49; an officer's narrative description of content observed during a previous device search, SUMF ¶¶ 33, 50, 51, 150; and a copy of data seized during a previous device search, SUMF ¶¶ 40, 41, 43. Defendants may share this information

with other law enforcement agencies. SUMF ¶¶ 14, 24. Defendants and other law enforcement agencies can place "lookouts" in TECS that flag travelers for additional scrutiny during future border crossings, which may include border searches of electronic devices. SUMF ¶¶ 27–32. ATS also may use information copied from travelers' devices in generating lookouts identifying travelers for heightened screening. SUMF ¶¶ 36, 37, 43.

CBP and ICE do not limit their searches of electronic devices to determining whether travelers are admissible to the United States or bringing in contraband. They claim authority to search travelers' devices for general law enforcement purposes, such as looking for potential evidence of illegal activity beyond violations of immigration and customs laws. SUMF ¶¶ 82, 83. That claimed authority extends to enforcing "hundreds" of federal laws, including tax, bankruptcy, environmental, and consumer protection laws. SUMF ¶¶ 81, 84. Defendants' asserted purposes for conducting warrantless or suspicionless device searches also include intelligence gathering or advancing pre-existing investigations, SUMF ¶¶ 86, 91, and Defendants consider requests from other government agencies to conduct device searches, SUMF at ¶¶ 87, 88. They may even conduct searches of electronic devices when the subject of interest is someone other than the traveler—such as when the traveler is a U.S. citizen and ICE is seeking information about a suspected undocumented immigrant; when the traveler is a journalist or scholar with foreign sources who are of interest to the U.S. government; or even when the traveler is the business partner of someone under investigation. SUMF ¶¶ 89, 90.

The number of border searches of travelers' devices is growing rapidly. CBP states that it searched 33,295 devices in fiscal year 2018, which is up nine percent from fiscal year 2017 (30,524), and up more than six-fold from fiscal year 2012 (5,085). SUMF ¶ 52. Due to lapses in record-keeping, these CBP figures are likely undercounts. SUMF ¶¶ 59–62. CBP also reports

hundreds of device confiscations per year. SUMF ¶ 55. ICE does not have aggregate data on its confiscations or basic searches. SUMF ¶¶ 56, 58. Despite the increasing frequency of the device searches they conduct, CBP and ICE do not know how many warrantless and suspicionless device searches uncover digital contraband or potential evidence of criminal activity. SUMF ¶¶ 99, 100.

LEGAL STANDARD

Summary judgment is appropriate where, as here, there is "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue exists only if specific facts—not conclusory allegations—would allow a judgment in the opposing party's favor. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248–49 (1986). After the movant has identified the basis for its motion, the nonmovant must identify specific facts that reveal a genuine issue for trial. *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986).

ARGUMENT

I. Warrantless, Suspicionless Searches of Electronic Devices at the Border Violate the Fourth Amendment

The unprecedented privacy interests Plaintiffs possess in the contents of their cell phones, laptops, and other personal electronic devices make warrantless, suspicionless border searches of those devices unconstitutional. As the Supreme Court held in *Riley*, electronic devices are unlike any other physical containers, given their "immense storage capacity" and the "highly personal" information they contain. 573 U.S. at 393, 395. *See also United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013), *aff'd*, *Riley*, 573 U.S. 373.

The Fourth Amendment's warrant requirement was enacted precisely to safeguard these kinds of privacy interests. Otherwise, the government would have unfettered access to "a virtual warehouse" of the most intimate aspects of Plaintiffs' lives, *Wurie*, 728 F.3d at 9, simply because

they travel abroad. *Carpenter* reinforced *Riley*, holding that searches of historical cell-site location information require a warrant, given the sensitivity of such records of a person's past movements. *See* 138 S. Ct. at 2223. Citing *Riley*, the *Carpenter* Court explained: "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." 138 S. Ct. at 2222.

Riley, *Carpenter*, and the Supreme Court's border-related decisions support the conclusion that border searches of electronic devices require a warrant. At a minimum, border searches of electronic devices require a heightened standard of suspicion that should apply to all such device searches, without distinguishing between methods of search.

A. Application of the Fourth Amendment Balancing Test in *Riley v. California* Dictates That a Warrant Is Required

In denying Defendants' motion to dismiss, this Court considered whether and how to apply *Riley*. Mem. Ord. at 35–36 ("[T]he Court is not persuaded that *Riley*'s reasoning is irrelevant here simply because *Riley*'s holding was limited to the search incident to arrest exception . . . . The reasoning in *Riley* may . . . carry some persuasive weight in the border search context."). As *Riley* reiterated, in determining whether to apply an existing warrant exception to a "particular category of effects"—such as cell phones—individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 573 U.S. at 385–86.[2] *See also* Mem. Ord. at 31–32.

Riley held that the search-incident-to-arrest exception to the warrant and probable cause requirements does not apply to cell phones for two reasons: first, individuals have unique privacy interests in the contents of cell phones; and second, warrantless, suspicionless searches of cell

[2] The Supreme Court has recognized the similarity between the border search exception and the search-incident-to-arrest exception. *See United States v. Ramsey*, 431 U.S. 606, 621 (1977). *See also* Mem. Ord. at 35.

phones are not sufficiently "tethered" to the underlying rationales for that exception, because they are not necessary to ensure officer safety or preserve evidence. *See Riley*, 573 U.S. at 385–86. *See also Wurie*, 728 F.3d at 13 (holding warrantless phone searches not "necessary" to advance the goals of the search-incident-to-arrest exception). Similarly, the border search exception should not apply to searches of travelers' electronic devices. The record shows that travelers' privacy interests outweigh any governmental interests, and thus the Fourth Amendment requires the government to obtain a warrant based on probable cause before searching travelers' electronic devices at the border.[3]

1. Travelers Have Extraordinary Privacy Interests in the Massive Quantities of Highly Personal Digital Data Their Electronic Devices Contain

The magnitude of the privacy interests at issue here is without compare. Border searches of personal property, like searches incident to arrest, are usually "limited by physical realities and tend[] as a general matter to constitute only a narrow intrusion on privacy." *See Riley*, 573 U.S. at 393. But searches of modern electronic devices, whether following an arrest or at the border, reveal the "sum of an individual's private life," *id.* at 394, and "bear[] little resemblance" to searches of bags, *see id.* at 386. *See also Wurie*, 728 F.3d at 9 ("[I]ndividuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, [or] briefcase."); *United States v. Kim*, 103 F. Supp. 3d 32, 55 (D.D.C. 2015). The fact that luggage at the border may contain some physical items with personal information does not negate the vast and unique privacy interests individuals have in electronic devices. *See Riley*, 573 U.S. at 400.

[3] This Court recognized that *Riley* "rejected the reasonable suspicion standard when it came to cell phone searches because it 'would prove no practical limit at all'" and that "[d]igital device searches at the border, perhaps even supported by reasonable suspicion, raise the same concerns." Mem. Ord. at 45.

Riley held that electronic devices differ fundamentally—in quantitative and qualitative senses—from physical containers. *Id*. at 393. However, the privacy interests that travelers have in the contents of their electronic devices today are likely greater than those in *Riley* because of continuing advances in the volume and type of data contained on devices and the ease with which CBP and ICE can quickly search them. *See id*. at 394 ("We expect that the gulf between physical practicability [of analog containers] and digital capacity [of electronic devices] will only continue to widen in the future.").

Quantitatively, with their "immense storage capacity," electronic devices can contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Id*. at 393–94. *See also United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) ("The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library."); SUMF ¶ 63.

Qualitatively, electronic devices contain information "of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." *Wurie*, 728 F.3d at 8. *See also* SUMF ¶ 64. Electronic devices "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. This data can easily reveal our political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. *Id*. at 395–96. These devices "not only contain[] in digital form many sensitive records previously found in the home; [they] also contain[] a broad array of private information never found in a home in any form—unless the phone is." *Id*. at 396–97. *See also Cotterman*, 709 F.3d at 964 (electronic devices "are simultaneously offices and personal diaries"

and "contain the most intimate details of our lives"). The Court in *Carpenter* required a warrant for one category of highly sensitive information—historical cell site location information—because "an individual maintains a legitimate expectation of privacy in the record of his physical movements." 138 S. Ct. at 2217. Many electronic devices contain a record of an individual's locations along with an array of other data. SUMF ¶ 69.

Additionally, the Supreme Court has long underscored the importance of evaluating privacy interests in the context of border searches. In *United States v. Ramsey*, the Court distinguished the search of a vessel or container from the search of a house: the latter required a warrant since before the ratification of the Constitution, even when conducted for purposes of enforcing customs laws, while the former typically did not, because "a port of entry is not a traveler's home." 431 U.S. 606, 617, 618 (1977) (citation omitted). *See also* 19 U.S.C. § 1595(a) (requiring warrant for customs searches of homes). But a search of a cell phone "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396 (emphasis in original).

Further, *Riley* required a warrant to search the cell phones of arrestees, who the Court stated have "diminished privacy interests." *Id*. at 392. Thus, even at the border, where a "traveler's privacy interests are ordinarily reduced," Mem. Ord. at 42, "*Riley* indicates that electronic devices implicate privacy interests in a fundamentally different manner than searches of typical containers or even searches of a person," *id*. The vast majority of international travelers are not suspected of any crime and thus have at least the privacy interests of arrestees.

The record in this case reinforces the extraordinary privacy interests at stake and the ease with which the government can invade them. The electronic devices that travelers carry across the border, including smartphones and laptops, can contain a very large volume of information,

SUMF ¶ 63, including photos, contacts, emails, and texts, SUMF ¶ 64. Indeed, the devices that Plaintiffs were carrying had enormous storage capacities, SUMF ¶¶ 121, 123, 125, 127, 129, 132, 134, 135, 137, 140–142, 144, 146, 149 (device types carried by Plaintiffs), and contained highly personal information, SUMF ¶¶ 122, 129, 139, 142. For example, Zainab Merchant and Nadia Alasaad both wear headscarves in public for religious reasons, and their devices contained photos of themselves without headscarves. SUMF ¶¶ 122, 139. Likewise, Merchant's device contained attorney-client privileged communications, which a CBP officer viewed over her objections, after the instant case was filed. SUMF ¶ 142. Jérémie Dupin used his searched device for his journalism work. SUMF ¶ 129.

Defendants can easily access this array of private information through border searches of electronic devices. When CBP or ICE conducts "basic" or manual searches of electronic devices, they can use the native search functions on the devices, including keyword search tools, to view files, images, or other information resident on the devices and accessible using their operating systems. SUMF ¶¶ 67–71. The content that may be searched includes information from the internet that is cached on a traveler's device. SUMF ¶ 75. Basic searches can even extend to metadata, such as the date and time associated with content, usage history, sender and receiver information, or location. SUMF ¶ 69. "Advanced" or forensic searches can reveal everything basic searches reveal, and sometimes deleted, password-protected, or encrypted data. SUMF ¶¶ 72, 73. Advanced searches may also copy all information on a device. SUMF ¶ 74.

CBP and ICE recognize the sensitivity of electronic device searches. SUMF ¶¶ 63, 65, 66. The privacy risks that border searches of electronic devices pose to travelers are compounded by the fact that information gleaned from a device may be shared with other federal agencies, as well as state, local, and foreign governments. SUMF ¶¶ 14, 24. CBP does not know how long

other government entities keep the information they receive from CBP's border device searches. SUMF ¶ 15.

In sum, travelers' devices contain an extraordinary amount of highly personal information that the government can easily search, retain, and share.

2. Warrantless, Suspicionless Device Searches Do Not Sufficiently Advance the Narrow Purposes of the Border Search Exception

The second prong of the Fourth Amendment balancing test evaluates the governmental interests by considering whether warrantless, suspicionless searches of the category of property at issue are tethered to the narrow rationales justifying the warrant exception. *See Riley*, 573 U.S. at 386. *See also Collins v. Virginia*, 138 S. Ct. 1663, 1671–72 (2018) (a warrantless search must not be "untether[ed]" from "the justifications underlying it") (quotation marks omitted); *Florida v. Royer*, 460 U.S. 491, 500 (1983) (warrantless searches "must be limited in scope to that which is justified by the particular purposes served by the exception"); *Wurie*, 728 F.3d at 9 (warrantless searches must be "commensurate" with the purposes of the exception); *Cotterman*, 709 F.3d at 956 (emphasizing "narrow" scope of border search exception).

Here, warrantless, suspicionless searches of electronic devices are not sufficiently tethered to the narrow purposes justifying the border search exception: immigration and customs enforcement, with a particular focus on the collection of duties and the interdiction of contraband. *See* Mem. Ord. at 39 (power to regulate "the collection of duties" and to prevent "the introduction of contraband" or "anything harmful" such as "communicable diseases, narcotics, or explosives" (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 537, 544 (1985))). *See also United States v. Soto-Soto*, 598 F.2d 545, 549 (9th Cir. 1979) ("Congress and the courts have specifically narrowed the border searches to searches conducted by customs officials *in enforcement of customs laws.*") (emphasis added). Border officers determine a traveler's

immigration status and authority to enter the United States by questioning travelers and inspecting official documents such as passports and visas, and they enforce customs laws by searching travelers' luggage, vehicles, and, if necessary, their persons. *See, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004); *United States v. Molina-Gomez*, 781 F.3d 13, 16–17 (1st Cir. 2015). The enforcement of immigration and customs laws does not justify unfettered access to travelers' electronic devices.

a. Defendants Conduct Warrantless, Suspicionless Device Searches for Evidence Gathering, a Purpose That Is Untethered from the Rationales Justifying the Border Search Exception.

The record shows that Defendants conduct warrantless, suspicionless electronic device searches for reasons far beyond those justifying the border search exception. Specifically, Defendants search electronic devices at the border for potential evidence. SUMF ¶ 91. *See also* Mem. Ord. at 34 (stating that the First Circuit in *Wurie* "found no Supreme Court jurisprudence sanctioning such a general evidence-gathering search") (internal quotation marks and citation omitted); *Kim*, 103 F. Supp. 3d at 59 (in granting the motion to suppress, stating that a laptop search was "for the purpose of gathering evidence in a pre-existing investigation" and "was so invasive of Kim's privacy and so disconnected from . . . the considerations underlying the breadth of the government's authority to search at the border . . . .").

First, Defendants' searches for evidence are not confined to possible violations of immigration and customs laws, making these searches completely untethered from the border search exception. Defendants conduct warrantless, suspicionless device searches to gather potential evidence of unlawful conduct with no nexus at all to the admissibility of people and goods. SUMF ¶¶ 81–83, 87, 88. Defendants assert authority to gather evidence about a wide range of law enforcement matters, including evidence about potential violations of financial, tax, environmental, consumer protection, or other laws—all without a warrant, probable cause, or any

individualized suspicion at all. SUMF ¶ 84. Defendants conduct warrantless, suspicionless searches of electronic devices for intelligence gathering, SUMF ¶ 86, and even search the devices of travelers who are not suspected of any wrongdoing, in order to gather potential evidence about other people, SUMF ¶¶ 89–90.

Second, Defendants' stated goal of finding potential *evidence* of customs violations, SUMF ¶ 85, is at most weakly tethered to the focus of the border search exception, which is on finding taxable or prohibited goods themselves (particularly where, as here, admissibility is not at issue for U.S. citizens and lawful permanent residents, *see* SUMF ¶ 2). As this Court held, mere "*information regarding* the inadmissibility of prohibited goods or persons . . . is distinct from contraband" itself. Mem. Ord. at 40 (emphasis added). This Court also invoked *United States v. Boyd* for the proposition that "search and seizure of 'goods liable to duties and concealed to avoid the payment thereof [] are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him.'" Mem. Order at 40 (quoting *Boyd*, 116 U.S. 616, 623 (1886)).[4]

[4] After *Riley*, other judges recognized this critical distinction between contraband itself and potential evidence of contraband. In *United States v. Molina-Isidoro*, Fifth Circuit Judge Costa, in a concurring opinion, was skeptical of a new "evidence-gathering justification" to support warrantless, suspicionless border searches of electronic devices. He explained that *Boyd*'s "emphatic distinction between the sovereign's historic interest in *seizing imported contraband and its lesser interest in seizing records revealing unlawful importation* has potential ramifications for the application of the border-search authority to electronic data that cannot conceal contraband and that, to a much greater degree than the papers in *Boyd*, contains information that is like an extension of the individual's mind." 884 F.3d 287, 297 (5th Cir. 2018) (Costa, J., specially concurring) (emphasis added). Similarly, in *United States v. Vergara*, Eleventh Circuit Judge J. Pryor, in a dissent, concluded that a forensic search of a device at the border requires a warrant and that a "general law enforcement justification" does not support warrantless, suspicionless device searches. 884 F.3d 1309, 1317 (11th Cir. 2018) (J. Pryor, J., dissenting). That such searches "may produce evidence helpful in future criminal investigations would thus 'untether the rule from [its] justifications.'" *Id. See also United States v. Kolsuz*, 185

Despite this distinction between evidence and the goods themselves, Defendants search electronic devices for information that could only be evidence—such as contact lists, location data, usage history, or other metadata. *See* SUMF ¶ 69, 72.

b. Warrantless, Suspicionless Device Searches Do Not Sufficiently Advance the Government's Stated Goals of Interdicting Physical and Digital Contraband, and Thus Are Untethered from the Border Search Exception.

As with the search-incident-to-arrest exception, where warrantless, suspicionless searches of a person are justified by the limited goals of protecting officer safety and preventing evidence destruction, the border search exception may "strike[] the appropriate balance in the context of physical objects" such as luggage, but its underlying rationales lack "much force with respect to digital content on cell phones" or other devices. *Cf. Riley*, 573 U.S. at 386. Just as the *Riley* Court stated that "data on the phone can endanger no one," *id*. at 387, physical items subject to customs laws cannot be hidden in digital data.

Since *Riley*, judges have recognized this weak tethering between conducting warrantless, suspicionless border searches of electronic devices and the interdiction of physical contraband in particular. In *Molina-Isidoro*, Judge Costa stated that the "[d]etection of … contraband is the strongest historic rationale for the border-search exception," yet "[m]ost contraband, the drugs in this case being an example, cannot be stored within the data of a cell phone," and so the "detection-of-contraband justification would not seem to apply to an electronic search of a cell phone or computer." 884 F.3d at 295 (Costa, J., specially concurring). And in *Vergara*, Judge J. Pryor similarly concluded: "the rationales underlying the border search exception lose force when applied to forensic cell phone searches," because "cell phones do not contain the physical

---

F. Supp. 3d 843, 858 (E.D. Va. 2016) (digital data "is merely indirect evidence of the things an individual seeks to export illegally—not the things themselves").

contraband that border searches traditionally have prevented from crossing the border." 884 F.3d at 1317 (J. Pryor, J., dissenting).

The limited digital content that is unlawful in and of itself does not justify warrantless, suspicionless device searches at the border. Child pornography, for instance, can be considered digital "contraband" that may be interdicted at the border. *Cf. United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376–77 (1971). But even to the extent that "[d]igital contraband like child pornography . . . falls within the ambit of the border search exception's rationales," Mem. Ord. at 40, warrantless, suspicionless device searches for such content remain insufficiently tethered to the border search exception. This is because, unlike physical contraband, digital contraband is primarily transported across borders via the internet, not ports of entry. SUMF ¶¶ 92, 95–97. *See also* Mem. Ord. at 41 ("[T]he vast majority of child pornography offenders today use the Internet or Internet-related technologies to access and distribute child pornography.") (quoting U.S. Sent'g Comm'n, *Federal Child Pornography Offenses* (2012)); *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting) ("electronic contraband is borderless").

Notably, CBP and ICE do not know how many warrantless or suspicionless searches of devices uncover digital contraband. SUMF ¶ 99. *See also* SUMF ¶¶ 101, 102 (CBP and ICE do not know how many device searches result in arrests, prosecutions, or convictions). Defendants therefore have no evidence that warrantless, suspicionless device searches are even effective at uncovering digital contraband, irrespective of whether such contraband is already available on the internet. *Cf. Riley*, 573 U.S. at 388–90 (finding insufficient evidence that warrantless searches of arrestees' phones would protect officer safety or prevent evidence destruction, and that any such possibilities do "not justify dispensing with the warrant requirement across the board"). Even when Defendants confiscate digital contraband at the border, they generally

cannot determine whether that digital contraband is already present in the United States, and at most they are sometimes able to use a digital "hashing" tool to determine that the contraband *is* already present in the United States. SUMF ¶ 98. Thus, the government cannot demonstrate that any digital contraband that might be physically resident on travelers' devices is a significant or "prevalent" problem *at the border*, or that the ability to conduct warrantless, suspicionless device searches "would make much of a difference" in preventing its entry into the country. *See Riley*, 573 U.S. at 389–90. *See also* Mem. Ord. at 32; *Cotterman*, 709 F.3d at 966 ("[L]egitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information.").

In short, the fact that some travelers' devices might contain one of the few types of data that constitute digital contraband, SUMF ¶ 93, 94, does not justify a *categorical rule* permitting warrantless, suspicionless searches of the devices of every traveler entering or exiting the country.

c. A Warrant Requirement for Device Searches at the Border Would Not Materially Impede Immigration and Customs Enforcement.

Defendants also cannot demonstrate that a warrant requirement "would impede customs officers' ability to ferret out such [digital] contraband." Mem. Ord. at 41. Where border officers have probable cause to believe contraband data is on a device, they can secure a search warrant.

CBP and ICE officers have experience in obtaining warrants for searches of electronic devices. SUMF ¶¶ 103, 110, 114. CBP and ICE also have policies regarding obtaining warrants in a variety of other contexts: to search international mail, subject travelers to body-cavity and x-ray searches, and detain travelers for longer than eight hours. SUMF ¶¶ 105–115. Defendants must always have a warrant to open certain international mail (outgoing parcels weighing less than a pound or sealed incoming mail that appears to only contain correspondence), and to read

correspondence in any incoming or outgoing international mail. SUMF ¶¶ 106, 113. ICE also needs a warrant to search correspondence on digital media located in international mail, SUMF ¶ 114, creating inconsistent procedures depending on whether a traveler brings a device to the border on their person as opposed to sending it through the mail.

Nor is the process of getting a warrant unduly burdensome. As the Supreme Court found in *Riley*, "[r]ecent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient." 573 U.S. at 401. Moreover, getting a warrant need not impede the efficient processing of travelers at the border. If border officers have probable cause to search a device, they may confiscate it and let the traveler continue on their way, then get a search warrant. *See infra* Part II. Defendants' policies already permit confiscation of devices after a traveler leaves the border, SUMF ¶ 11, 21, and there is no suggestion that they cannot thereafter get a warrant in a reasonable time period. In instances where there is truly no time to go to a judge, the exigent circumstances exception may apply on a case-by-case basis. *See Riley*, 573 U.S. at 388.

As this Court stated, "the government's interests—even if they are not 'untethered' to the exception's rationales—must be weighed against the significant privacy implications inherent in cell phone data searches." Mem. Ord. at 41–42 (internal quotation marks and citation omitted). Even assuming that warrantless, suspicionless device searches at the border might sometimes help with immigration and customs enforcement, the extraordinary privacy interests that travelers have in their digital data outweigh any government interests. As a result, the Fourth Amendment requires border officers to obtain a warrant before searching electronic devices.

B. Warrantless, Suspicionless Border Searches of Electronic Devices Are Unreasonable Under the Fourth Amendment

Border search cases provide a parallel justification for requiring a warrant for border searches of electronic devices. The Supreme Court has held that the scope of the border search

exception to the warrant requirement is limited, and that "[t]he Fourth Amendment commands that searches and seizures [at the border] be reasonable." *Montoya de Hernandez*, 473 U.S. at 537. As in other contexts, "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." *Id*. For example, the Court has left "open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive manner in which it is carried out.'" *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13). Lower courts also have recognized that particularly "intrusive" or "offensive" searches at the border may "be deemed unreasonable under the Fourth Amendment." *See, e.g., United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008).

Warrantless, suspicionless device searches at the border are unreasonable because they invade substantial privacy interests. They also raise grave First Amendment concerns that affect the reasonableness analysis. *See infra* Part III. In *Ramsey*, the Court left open the possibility that where border searches burden First Amendment rights, the "full panoply" of Fourth Amendment protections—*i.e.* a warrant requirement—might apply. 431 U.S. at 623–24 & n.18.

C. At a Minimum, the Fourth Amendment Requires A Heightened Standard of Suspicion for Border Searches of Electronic Devices

If this Court holds that no warrant is required for border searches of electronic devices, it should hold they require probable cause. *Cf. California v. Acevedo*, 500 U.S. 565, 579–80 (1991) (although automobile searches do not require a warrant, they do require probable cause). A probable cause threshold is necessary to limit the massive privacy intrusion of such searches. *Cf. id.* at 574–76. The Supreme Court has never suggested that the reasonable suspicion it required in *Montoya de Hernandez* is a ceiling for every kind of border search. 473 U.S. at 541 n.4 (declining to decide "what level of suspicion" is required for highly intrusive searches); *Flores-*

Montano, 541 U.S. at 152. Additionally, as this Court has recognized, "[t]he Supreme Court has not explicitly held that all property searches" at the border never require suspicion. *House v. Napolitano*, 2012 WL 1038816, *7 (D. Mass. 2012). More recently, the Fourth Circuit in *United States v. Kolsuz* held that forensic device searches at the border require *some* level of individualized suspicion and left open the possibility that a warrant could be required. 890 F.3d 133, 137 (4th Cir. 2018).

At the very least, courts have required reasonable suspicion for certain "non-routine" border searches. *See Montoya de Hernandez*, 473 U.S. at 541 n.4 (requiring reasonable suspicion for the non-routine detention of a suspected alimentary canal smuggler for a lengthy period). *See also Flores-Montano*, 541 U.S. at 152 (singling out "highly intrusive searches" that impact the "dignity and privacy interests" of travelers); *United States v. Braks*, 842 F.2d 509, 511, 512 n.12 (1st Cir. 1988) (determining whether a border search is routine or non-routine by analyzing a search's "degree of invasiveness or intrusiveness," with one factor being whether it abrogates reasonable expectations of privacy).[5] Defendants already apply a reasonable suspicion standard to a variety of searches at the border. SUMF ¶¶ 116–119. *See also* 19 U.S.C. § 482(a) ("reasonable cause" required for customs searches of "any trunk or envelope"). They could easily do so for all border device searches.

[5] The First Circuit in *Braks*, 842 F.2d at 511, 512 n.12, rested on *Winston v. Lee*, 470 U.S. 753, 762 (1985), which provided examples of intrusions (such as eavesdropping and home searches) that are not bodily intrusions but nonetheless "damage the individual's sense of personal privacy and security." Device searches are more intrusive than these *Winston* examples: they reveal "far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396 (emphasis in original). Indeed, this Court was correct to state that *Riley* and *Wurie* "indicate that electronic device searches are, categorically, more intrusive than searches of one's person." Mem. Ord. at 43.

D. There is No Valid Distinction Between Manual and Forensic Device Searches at the Border

Before *Riley*, the Ninth Circuit in *Cotterman* required reasonable suspicion for a forensic search but none for a manual search. 709 F.3d at 967–68. Defendants' policies also distinguish between manual ("basic") and forensic ("advanced") searches. SUMF ¶¶ 9, 10, 18, 19.

This distinction is legally and technologically untenable. Both manual and forensic searches severely harm individual privacy by accessing essentially the same trove of highly personal information. Given the increasing volume and detail of data electronic devices contain, and the growing ease of manually navigating them, manual searches are extraordinarily invasive of travelers' privacy. SUMF ¶¶ 68–71. Without special training or equipment, a border officer can easily open and peruse myriad stored files, programs, and apps, and do so with a device's own built-in search function allowing the officer to search for particular words and images. SUMF ¶¶ 70, 71. Indeed, the unconstitutional warrantless cell phone searches in *Riley* were manual. *See* 573 U.S. at 379–80, 400. *See also Kim*, 103 F. Supp. 3d at 55 (the reasonableness of a border device search does not "turn on the application of an undefined term like 'forensic'").[6] Thus, if this Court decides that border searches of electronic devices require a warrant and/or a heightened standard of suspicion, it should extend that protection to all searches, not just forensic searches.

[6] Even when a phone is disconnected from the internet, border officers can still view information that originated on the internet and has been "cached" on the device. SUMF ¶ 75. Moreover, CBP policy prohibits accessing live cloud-based content, but some CBP officers may have accessed cloud-based content during searches of electronic devices, even after issuance of an April 2017 memorandum requiring that officers disable network connectivity prior to search. SUMF ¶ 76. *Riley* weighed the additional privacy harms of potential cloud searches, even if government "protocols" would prohibit them. 573 U.S. at 398.

II. Absent Probable Cause, Confiscations of Electronic Devices After a Traveler Has Left the Border Violate the Fourth Amendment

The Fourth Amendment requires all seizures to be justified at their inception and reasonable in scope and duration. *See United States v. Place*, 462 U.S. 696, 701, 709–10 (1983). Thus, confiscation of a device after a traveler leaves the border must be based on at least the level of suspicion needed for the subsequent search—in this case, probable cause (as required to get a warrant). *See supra* Part I.A. Any lesser standard is unreasonable, because it would permit confiscations where a subsequent search is not permitted. *Place*, 462 U.S. at 701 ("Where . . . authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the [Fourth] Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents.").

Additionally, the duration of all seizures must be reasonable. *See House*, 2012 WL 1038816, at *9 (discussing *Place*, and holding that a 49-day border seizure of electronic devices raised a plausible claim). When determining the level of suspicion necessary to justify a seizure at its inception, the duration is an "important factor." *See Place*, 462 U.S. at 709. In *Place*, the Court held that the detention of a domestic traveler's luggage for 90 minutes without probable cause violated the Fourth Amendment. *Id*. at 708. *See also United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (holding that a 21-day delay in securing a warrant for a computer search was unreasonable, because computers are indispensable in everyday life). In the border context, courts likewise consider the length of a device seizure to determine its reasonableness. *See Molina-Gomez*, 781 F.3d at 20 (suggesting that reasonable suspicion was required for a 22-day confiscation).

Defendants' policies do not satisfy these requirements. They permit confiscations of electronic devices after a traveler has left the border absent probable cause (and often absent any

suspicion at all), and they lack any effective limit on the duration of such confiscations. SUMF ¶¶ 11, 12, 21. Plaintiffs' experiences are illustrative. Without probable cause, Defendants effected prolonged confiscations of the devices of Plaintiffs Ghassan and Nadia Alasaad (approximately 12 days), SUMF ¶ 121, 154, Suhaib Allababidi (over 10 months for one device and over two months for a second one), SUMF ¶¶ 160, 161, and Wright (56 days), SUMF ¶ 166.

III. Warrantless, Suspicionless Searches of Electronic Devices Violate the First Amendment

Defendants violate the First Amendment by searching and seizing the contents of electronic devices at the border without a warrant or even individualized suspicion. Such devices include highly sensitive information concerning Plaintiffs' personal, privileged, confidential, and anonymous communications and associations. SUMF ¶¶ 122, 139, 142.

Government demands for information revealing expressive activities burden First Amendment rights and require significant protections. *See, e.g., Gibson v. Florida Legis. Investigation Comm.*, 372 U.S. 539, 544 (1963). The government must have a compelling interest in the information and must not seek more information than necessary. *See, e.g., id.* at 546 (prohibiting a legislative subpoena to the NAACP); *United States v. Rumely*, 345 U.S. 41, 46 (1953) (prohibiting a congressional subpoena to a bookseller seeking names of purchasers of political publications); *Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972) (requiring substantial and immediate government interests in the information sought by a grand jury about a newspaper, and a means of obtaining it that was "not more drastic than necessary").

Here, Defendants' device searches violate many First Amendment rights, including: (1) the "freedom to engage in association for the advancement of beliefs and ideas," confidentially and without government scrutiny, *NAACP v. Alabama*, 357 U.S. 449, 460 (1958); (2) the right to speak anonymously, including online, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357

(1995); *McMann v. Doe*, 460 F. Supp. 2d 259, 266 (D. Mass. 2006); (3) the right to receive and communicate unpopular ideas, confidentially and without government scrutiny, *Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965); (4) the right to read books and watch movies privately, *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167–70 (W.D. Wash. 2010); *In re Grand Jury*, 706 F. Supp. 2d 11, 17–18 (D.D.C. 2009); and (5) the right to gather and publish newsworthy information absent unfettered government access to the identity of sources and journalistic work product, *Branzburg v. Hayes*, 408 U.S. 665, 709 (1972) (Powell, J., concurring); *Bruno & Stillman, Inc. v. Globe Newspaper Co.*, 633 F.2d 583, 595–96 (1st Cir. 1980).

As this Court noted, Defendants have not argued "that warrantless searches would not be a significant or substantial burden on travelers' First Amendment rights." Mem. Ord. at 49. Nor could they, given the quantity and quality of information such searches yield to government agents, *see supra* Part I.A.1, and the fact that Plaintiffs include journalists whose sources and journalistic work product may have been exposed, SUMF ¶¶ 128–130, 133.

When searches burden First Amendment rights, a warrant is required. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that First Amendment interests should be protected by applying Fourth Amendment warrant standards with "scrupulous exactitude"); *New York v. P.J. Video, Inc.*, 475 U.S. 868, 877–78 (1986) (holding that a warrant was an adequate constitutional safeguard for a search of expressive materials).[7]

[7] *See also* Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Natl. Sec. L. & Policy 247, 249, 250 (2015) (the Fourth Amendment is tied to the First Amendment, the "papers" clause protects expressive and associational data, and a warrant should be "the constitutional default"); Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 154, 159 (2007) (First Amendment procedural protections apply when there is a "chilling effect," and "a warrant supported by probable cause will, in most cases, suffice to satisfy the narrow tailoring requirement").

Moreover, there is no doubt that the First Amendment applies at the border. In *Ramsey*, the Court recognized that First Amendment-protected speech might be chilled by customs searches of incoming international mail. While the Court upheld the statutory search regime, it emphasized that regulations "flatly prohibit[ed], under all circumstances," the reading of correspondence without a warrant. 431 U.S. at 623. The Court explicitly left open whether, absent this safeguard, it would require "the full panoply of Fourth Amendment requirements." *Id*. at 624 n.18.

IV. Plaintiffs Have Standing to Seek Injunctive Relief

Plaintiffs' standing to seek prospective relief rests on two independent foundations. First, Plaintiffs suffer continuing harm from past border searches of their electronic devices—namely, the retention of information seized from their devices—and an expungement order will cure this harm. Second, Plaintiffs face substantial risk of future searches and confiscations, and an injunction and declaration against the challenged policies and practices will end this risk.

A. Plaintiffs Have Standing to Seek Expungement

This Court previously determined that "[e]xpungement is a remedy that falls within the Court's equitable discretion." Mem. Ord. at 27. *See, e.g., Peters v. Hobby*, 349 U.S. 331, 349 (1955) (expungement of employment records concerning employee's loyalty); *Callicotte v. Carlucci*, 731 F. Supp. 1119, 1120–21 (D.D.C. 1990) (expungement of employment records concerning discipline arising from disability); *United States v. Bohr*, 406 F. Supp. 1218, 1219–20 (E.D. Wisc. 1976) (expungement of arrest and indictment records).

"Retention of data illegally obtained by law enforcement may constitute continued harm sufficient to establish standing to seek expungement." Mem. Ord. at 24. This is because the "continuing, present adverse effects" of "past exposure to illegal conduct" can support standing. *O'Shea v. Littleton*, 414 U.S. 488, 495–96 (1974). Thus, when law enforcement improperly

collects information about a person, the continued retention of that information is an ongoing injury, and a demand to expunge it supports standing. *See Tabbaa v. Chertoff*, 509 F.3d 89, 96 n.2 (2d Cir. 2007) ("[P]laintiffs possess Article III standing based on their demand for expungement."); *Hedgepeth v. WMATA*, 386 F.3d 1148, 1152 (D.C. Cir. 2004).

Here, Plaintiffs seek expungement of personal information that Defendants unlawfully seized from their devices and continue to retain. Compl. at ¶ 157 & Prayer ¶ I. Each Plaintiff suffered at least one device search at the border. SUMF ¶¶ 120–149. Defendants' policies expressly authorize retention of data obtained from device searches. SUMF ¶¶ 13, 22; Mem. Ord. at 25–26. CBP and ICE officers are capable of making and retaining both (i) electronic copies of information seized from travelers' devices, and (ii) notes of what they observed inside the devices. SUMF ¶¶ 33, 40–41, 50. Defendants have produced incident reports documenting substantive content observed during searches of the devices of four Plaintiffs: the Alasaads, Dupin, and Akram Shibly. SUMF ¶ 150. Defendants admit they possess additional content from the devices of five Plaintiffs: Nadia Alasaad, Sidd Bikkannavar, Dupin, Merchant, and Diane Maye Zorri. *Id*. Defendants' records also show they maintain information from Matthew Wright's devices: officers extracted information from his devices; they did not document its destruction (though Defendants' policies require such documentation); and after returning the devices to Wright, officers transferred his data among government units. SUMF ¶ 151.

Finally, expungement will redress a serious harm. Defendants' ongoing retention of this information compounds the violations of Plaintiffs' constitutional rights, because Defendants remain free to retain it for a long time, use and exploit it, or share it with other agencies that may do the same. SUMF ¶¶ 42, 77–80 (CBP's 2018 policy at § 5.5.1.3–5.5.1.4). "[T]o the extent

Plaintiffs' information was copied or obtained, subsequently retained and not destroyed by CBP and ICE, the destruction of these copies or data could redress such injury." Mem. Ord. at 27.

B. Plaintiffs Also Have Standing Because the Record Confirms the Allegations This Court Relied On Regarding Likelihood of Future Search

To establish Article III standing, a plaintiff must show: (1) an "injury in fact" that is "concrete and particularized" and "actual or imminent," not "conjectural" or "hypothetical"; (2) a "causal connection" between the injury and the defendant's conduct; and (3) a likelihood that a favorable decision will "redress[]" the injury. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). For an injunction, a plaintiff must also show "a sufficient likelihood that he will again be wronged in a similar way." *Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983). This requires a "substantial risk" of harm *or* a threat that is "certainly impending." *Reddy v. Foster*, 845 F.3d 493, 500 (1st Cir. 2017) (quoting *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014)). *See also* Mem. Ord. at 17–18.

Plaintiffs face a substantial risk of future injury for two reasons. First, Plaintiffs will be exposed to Defendants' policies and practices whenever they travel abroad. Second, Plaintiffs suffer probabilistic injury.

Standing to obtain prospective relief may rest on proof that (1) the defendant adopted an unlawful policy or practice, and (2) the plaintiff will be exposed to it. *See Berner v. Delahanty*, 129 F.3d 20, 24 (1st Cir. 1997) (requiring "a realistic risk of future exposure to the challenged policy"). Injured parties can show future injury when, as here, "[t]he offending policy remains firmly in place." *Dudley v. Hannaford Bros. Co.*, 333 F.3d 299, 306 (1st Cir. 2003).

This Court held that Plaintiffs sufficiently alleged substantial risk of future harm. Mem. Ord. at 24. The Court emphasized that "Plaintiffs challenge policies that are in place and are being actively enforced," and that their "alleged future injury does not depend upon defendants'

future illegal conduct untethered to a pattern of past practice . . . but rather upon recurring conduct authorized by official policies." *See id*. at 20–21 (distinguishing *Lyons*).[8] This Court also explained that "all Plaintiffs have been subjected to electronics searches at the border and four Plaintiffs have been subjected to multiple device searches." *Id*. at 21.

This Court rejected Defendants' argument that Plaintiffs lack standing because 0.008% of travelers were subjected to border device searches during a particular period. *Id*. at 19. The Court reasoned that "there is no numerical threshold . . . at which likelihood of harm becomes a 'substantial risk' of harm," *id*. at 19, and that "30,000 searches per year is not a 'rare occurrence,'" *id*. at 20. This Court further held that "even a small probability of injury is sufficient to create a case or controversy" where "the relief sought would, if granted, reduce the probability." *Id*. at 20 (citing *Massachusetts v. EPA*, 549 U.S. 497, 525 n.23 (2007)). It further noted that the fact that "four Plaintiffs here have been subjected to multiple searches . . . suggests that the risk of future search is higher for these plaintiffs than the general population." *Id*. at 20.

This Court correctly emphasized the repeated searches of particular Plaintiffs. The "possibility of recurring injury ceases to be speculative when actual repeated incidents are documented." *Thomas v. City of Los Angeles*, 978 F.2d 504, 507 (9th Cir. 1992); *Floyd v. City of New York*, 283 F.R.D. 153, 169 (S.D.N.Y. 2012). *See, e.g., Stinson v. City of New York*, 282 F.R.D. 360, 382 (S.D.N.Y. 2012); *Smith v. City of Chicago*, 143 F. Supp. 3d 741, 752 (N. D. Ill. 2015); *Morales v. Chadbourne*, 996 F. Supp. 2d 19, 37–38 (D. R. I. 2014); *Cherri v. Mueller*, 951 F. Supp. 2d 918, 930 (E.D. Mich. 2013); *Aguilar v. ICE*, 811 F. Supp. 2d 803, 827 (S.D.N.Y. 2011).

[8] The Court properly distinguished *Lyons*. There, the plaintiff did not allege that the government "ordered or authorized" the challenged practice. 461 U.S. at 106. Many cases thusly distinguish *Lyons*. *See, e.g., Postal Union v. Frank*, 968 F.2d 1373 (1st Cir. 1992); *Connor B. v. Patrick*, 771 F. Supp. 2d 142, 153 (D. Mass. 2011); *Mack v. Suffolk Cty.*, 191 F.R.D. 16, 21 (D. Mass. 2000).

This Court was also correct to consider probabilistic standing. "[P]robabilistic harms are legally cognizable." *Maine People's All. v. Mallinckrodt, Inc.*, 471 F.3d 277, 282, 283, 285 (1st Cir. 2006). In other words, "threatened harm in the form of an increased risk of future injury" can establish standing. *Baur v. Veneman*, 325 F.3d 625, 633 (2d Cir. 2003). "[E]ven a small probability of injury is sufficient to create a case or controversy." *EPA*, 549 U.S. at 525 n.23. For example, plaintiffs had standing to challenge an emissions policy that created a 1 in 200,000 risk of skin cancer, *NRDC v. EPA*, 464 F.3d 1, 7 (D.C. Cir. 2006), and a drilling policy that created a 1 in 10,000 risk of an oil well fire, *Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 93 (D.D.C. 2006).[9]

Finally, this Court rejected Defendants' argument that Plaintiffs must name specific dates of future travel. Mem. Ord. at 22. It distinguished *Lujan*, because "exposure to CBP and ICE policy does not require travel to a specific destination, but rather only requires some international travel and return to the U.S.," and "Plaintiffs allege prior travel abroad and professional backgrounds that might warrant future travel." *Id*. at 22–23.

The summary judgment record confirms the allegations this Court relied on in its standing determination at the motion to dismiss stage:

- Defendants' policies and practices permit warrantless searches, and usually permit suspicionless searches, of travelers' electronic devices at the U.S. border. SUMF ¶¶ 9, 10, 18, 19.

[9] In *Abidor v Napolitano*, 990 F. Supp. 2d 260, 270–73 (E.D.N.Y. 2013), the court legally erred by rejecting the probabilistic approach. *Abidor* is also factually distinct. After that decision, the government dramatically expanded its program of border device searches, increasing the search odds from about 1-in-100,000 then, *id.* at 271, to about 1-in-10,000 now, *see* SUMF ¶ 52; Pls. Exh. 46 at ¶ 13. So where the *Abidor* court assumed Defendants would not search phones absent reasonable suspicion, due to a supposed lack of search resources, 990 F. Supp. 2d at 271–72, that assumption no longer holds.

- Each Plaintiff was subjected to at least one search, SUMF ¶¶ 120–149, and four suffered multiple searches: Merchant suffered four (three after filing suit), and Nadia Alasaad, Dupin, and Isma'il Kushkush each suffered at least two. SUMF ¶¶ 121, 123, 129, 130, 134, 135, 137, 140, 141, 142. Further, most Plaintiffs have been subjected to secondary inspection and border searches of their baggage multiple times. SUMF ¶¶ 167–168.
- CBP reported over 30,000 device searches in fiscal year 2017, and over 33,000 in fiscal year 2018. SUMF ¶ 52. Thus, searches *increased* beyond the number this Court determined was not "rare." *See* Mem. Ord. at 20. Because Defendants fail to track all searches, SUMF ¶¶ 56–62, the real numbers are likely higher. Searches are up six-fold from six years earlier. SUMF ¶ 52.
- All Plaintiffs intend to continue to travel abroad, SUMF ¶¶ 169–189, and some have purchased tickets or made specific plans to do so, SUMF ¶¶ 170, 172, 174, 176, 178, 182, 187, 189.
- Defendants' databases maintain records of Plaintiffs' past device searches. SUMF ¶¶ 5, 26, 34, 37, 49. These records sometimes include copies or descriptions of content from Plaintiffs' devices. SUMF ¶ 150–151. Border officers may access such records when Plaintiffs cross the border, and may rely on them when deciding whether to conduct another device search. SUMF ¶¶ 25, 35, 36, 44, 48. So Plaintiffs face a higher risk than the general public. *See* Mem. Ord. at 24. *See also Tabbaa v. Chertoff*, 2005 WL 3531828, *9 (W.D.N.Y. 2005).

CONCLUSION

For the foregoing reasons, Plaintiffs request summary judgment on all claims.

Respectfully submitted: Dated: April 30, 2019

Adam Schwartz *
Sophia Cope*
Saira Hussain*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 (phone)
(415) 436-9993 (fax)
adam@eff.org
sophia@eff.org
saira@eff.org

/s/Esha Bhandari
Esha Bhandari*
Hugh Handeyside*
Nathan Freed Wessler*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
(212) 549-2500 (phone)
(212) 549-2583 (fax)
ebhandari@aclu.org
hhandeyside@aclu.org
nwessler@aclu.org

Jessie J. Rossman
BBO #670685
Matthew R. Segal
BBO #654489
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
(617) 482-3170 (phone)
(617) 451-0009 (fax)
jrossman@aclum.org
msegal@aclum.org

*Admitted *pro hac vice*
Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I certify that on April 30, 2019, a copy of the foregoing was filed electronically via the Court's ECF system, which effects service upon counsel of record.

/s/ *Esha Bhandari*
Esha Bhandari